



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,363	03/15/2004	Jochen Weber	10191/3602	3174
26646	7590	11/07/2007		
KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004			EXAMINER TRAORE, FATOUMATA	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 11/07/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/801,363

Applicant(s)

WEBER ET AL.

Examiner

Fatoumata Traore

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 05 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. This is in response to the amendment filed on October 5<sup>th</sup>, 2007. Claims 1-19 are pending and have been considered below.

#### ***Claim Objections***

2. The amendment to claims 4 and 11 filed on October 5<sup>th</sup>, 2007 have been considered and effectively overcome the previous claim objection. Therefore, the previous claim objection has been withdrawn.

#### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 19, 10 and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Gilley et al (US 5,771,287).

***Claim 1:*** Gilley et al discloses an apparatus for controlling the feature set of a programmable device comprising:

- i. A plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non- exchangeable manner (AAC refers to a value which is calculated by using the SK of the scrambler and the OMC which has been authorized by

the factory and has been stored in EEPROM) (column 6, lines 9-12 Fig. 1 item 16);

ii. An arrangement for storing a code number, the code number being obtained from the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number (A secured encryption algorithm is used with the operation mode code and the secret key to create the authentication code) (column 5, line 65 to column 7 line 1),

iii. Wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison (This present authentication code is then compared by the programmable device to the factory calculated and set authentication code that was originally stored in the programmable device memory. If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable device can take a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set) (column 4, lines 22-34; column 7, lines 1-17).

**Claim 9:** Gilley et al discloses an apparatus for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 1 above, and further discloses that at least two of the modules are each identified by a serial number and the code number is obtained by joint encryption of the serial numbers (Both the EEPROM and ROM contain serial number SN) (column 6, lines 30-60, figure 1).

**Claim 10:** Gilley et al discloses a method for controlling the feature set of a programmable device comprising:

- i. Storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number (AAC refers to a value which is calculated by using the SK of the scrambler and the OMC which has been authorized by the factory and has been stored in EEPROM) (column 6, lines 9-12 Fig. 1 item 16);  
Reading the code number and calculating an unencrypted serial number from the code number with the aid of the information (the authentication code is calculated using the operation mode code and the secret key together with a cryptographic methodology. This authentication code is then also programmed in a programmable device's memory. It does not have to be secured) (column 4, lines 12-6);
- ii. Comparing the decrypted serial number thus obtained with the serial number of the module (This present authentication code is then

Art Unit: 2136

compared by the programmable device to the factory calculated and set authentication code that was originally stored in the programmable device memory) (column 4, lines 22-30); and

iii. Detecting an exchange of the module if the serial number of the module does not match the decrypted serial number (If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set) (column 4, lines 26-34; column 7, lines 1-17).

**Claim 17:** Gilley et al discloses a method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above, and further discloses that the method is used for a plurality of modules of the microprocessor system and the code number is obtained by a joint encryption of serial numbers of the plurality of modules the module includes a microprocessor of the microprocessor system (a secure encryption algorithm is used with the operation mode code and the secret key to create the authentication code) ( column 5, lines 66-67 and column 6 lines 1-5).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claim 2-8, 11-16, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilley et al (US 5,771,287) in view of Osborn (US 6,026,293).

**Claims 2, 11:** Gilley et al discloses a apparatus and method for controlling the feature set of a programmable device as in claims 1 and 10 above, but does not disclose that a asymmetric encryption method is used. However, Osborn discloses an apparatus for preventing tampering with memory in electronic device, which further discloses an asymmetric authentication (data transfer device authentication involves the use of a public/private key authentication scheme) (column 6, lines 50-53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add asymmetric encryption in Gilley et al. One would have been motivate to do so in order to maintain system security.

**Claims 3, 12:** Gilley et al and Osborn disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 2 and 10 above, and Gilley et al further discloses that one of the at least one module identified by the serial number is a storage module (figure 1).

**Claims 4, 13:** Gilley et al and Osborn disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 3 and 12 above, and Gilley et al further discloses that the code number is stored in a same storage module as the serial number (the read only memory contains the serial, the code to enable the scrambling function) (column 6, lines 53-57 and Figure 1).

**Claims 5, 14:** Gilley et al and Osborn disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 3 and 12 above, and Gilley et al further discloses that the storage module is an electrically rewritable, non-volatile memory (scrambler also utilizes an electrically erasable programmable read Only memory) (column 5, lines 31-3), and the code to be executed if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module ( If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set, other action are possible (deletion of storage module)) (column 4, lines 26-34).

**Claims 6, 15:** Gilley et al discloses an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 1 and 10 above, but does not explicitly disclose



that one of the at least one module identified by the serial number is the microprocessor. However, Osborn discloses an apparatus for preventing tampering with memory in electronic device, which further discloses a microprocessor as one of the module identified by the serial number (figure 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the step of identifying the microprocessor by the serial number in Gilley et al. One would have been motivate to do so in order to maintain system security.

**Claims 7, 16:** Gilley et al discloses an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 1 and 10 above, but does not explicitly disclose that the information required to calculate the serial number from the code number is stored in a different storage module than the code number. However, Osborn discloses an apparatus for preventing tampering with memory in electronic device, which further discloses that the information required to calculate the serial number from the code number is stored in a different storage module than the code number (the Internal Read Only Memory IROM contains boot code, hashing code, authentication code and public encryption key, The Electronically Erasable Programmable Read Only Memory (EEPROM) includes user profile data, and Electronic Serial Number (ESN) ( column 7 line 67 and column 8, lines 1-7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the step of storing the information

required to calculate the serial in a different module in Gilley et al. One would have been motivate to do so in order to maintain system security.

**Claim 8:** Gilley et al and Osborn disclose an apparatus for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 7 above, and Gilley et al further discloses the different storage module is connected to the microprocessor in a non-separable manner (scramble includes a microprocessor, an electrically erasable programmable read only memory and a read only memory) (column 5, lins29-35).

**Claim 18:** Gilley et al discloses an method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above, but does not explicitly disclose that steps of the method are executed upon each start-up of the microprocessor system. However, Osborn discloses an apparatus for preventing electronic memory tampering, which further discloses that the steps of the method are executed upon each start-up of the microprocessor system (A process for telephone power up and memory validation for the system depicted in Fig 4, according to an exemplary embodiment of the invention, is illustrated in Fig 5. After the cellular telephone is turned on, boot code within the Internal Read Only Memory (IROM) is executed by the microprocessor to initialize the controller. Has code containing in the IROM is then run to perform an audit hash value calculation over selected contents of the flash program and the Electronic Serial Number (ESN) value

Art Unit: 2136

stored in EEPROM) (column 8, lines 19-30). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the steps of execution of the method at each start-up in Gilley et al. One would have been motivate to do so in order to maintain system security.

**Claim 19:** Gilley et al discloses an method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above but does not explicitly disclose that steps of the method are periodically executed during operation of the microprocessor system. However, Osborn discloses an apparatus for preventing tampering with memory in electronic device, which further discloses that steps of the method are periodically executed during operation of the microprocessor system (a periodic hash value calculation process is enabled, where after the cellular telephone begins normal operation) (column 8, lines 38-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the steps of a periodical execution of the method in Gilley et al. One would have been motivate to do so in order to maintain system security.

### ***Response to Arguments***

7. Applicant's arguments filed October 5<sup>th</sup>, 2007 have been fully considered but they are not persuasive.

a. ***Regarding Claim 1 and 10:*** Applicant argued that "nothing in Gilley actually teaches or suggest the above-recited claimed features of claims 1 and

Art Unit: 2136

10, in particular the claimed feature that "the microprocessor is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison." However, the examiner respectfully disagrees and submits that Gilley et al in fact discloses that the microprocessor is adapted to calculate a serial number (a present authentication code)(column 6, lines 18-22) from the code number (secret key) on the basis of the information (column 6, lines 18-22), to compare the calculated serial number (present authentication code (PAC)) to the stored serial number (authorized authentication code AAC), and to execute or not execute at least part of the code as a function of a result of the comparison(the programmable device can take a number of different actions including refusing to conduct certain functions, refusing to operate at all , or defaulting to a lower feature set) (column 4, lines 22-33; column 7 , lines 1-17).

b. **Regarding claims 9 and 17:** Applicant has no remarks.

c. **Regarding Claims 2-8, 1-16, 18 and 19:** The applicant remarks regarding these claims have already been discussed above.

8. There is no new ground of rejection when the basic thrust of the rejection remains the same. See *In re Kronig*, 539 F.2d 1300, 1302-03, 190 USPQ 425, 426-27 (CCPA 1976) To the extent that the response to the applicant's arguments may have mentioned new portions of the prior art references, which were not used in the prior

Art Unit: 2136

office action, this does not constitute new a new ground of rejection. It is clear that the prior art reference is of record and has been considered entirely by applicant. See *In re Boyer*, 363 F.2d 455,458 n.2,150 USPQ 441,444, n.2 (CCPA 1966) and *In re Bush*, 296 F.2d 491,496, 131 USPQ 263,267 (CCPA 1961).

The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. *In re Meinhardt*, 392, F.2d 273,280, 157 USPQ 270, 275 (CCPA 1968).

Accordingly, this office action is being made final.

Therefore, the examiner submits that the combined teaching of Gilley et al and Osborn discloses each and every feature of the above claims and respectfully maintains the rejection.

### ***Conclusion***

**9. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2136


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT  
Monday November 5<sup>th</sup>, 2007

Nassar G. Moazzami  
Supervisory Patent Examiner

  
111 5,07